UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,611	03/31/2000	Carl M. Ellison	042390.P8112	2172

8791   7590   08/10/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER
TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION. ·
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 19 May 2005.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) 61-90 is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) 61-90 is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to communication: 19 May 2005, with an original filing date of

31 March 2000.

2.   Claims 1-60 have been canceled by amendment. Claims 61, 71, and 80 have been

amended.

3.   Claims 61-90 are currently pending in this application. Claims 61, 71, and 81 are

independent claims.

Response to Arguments

4.   Applicant's arguments with respect to anticipated rejection have been considered but are

not persuasive.

With respect to applicant's first argument on page 12, "By contrast, claim 81 in the

present application recites a processing system comprising a processor that supports "a normal

execution mode in a ring O operating mode". The amendment to the claims adding "a ring O"

does not change the meaning of the claim, which was rejected in previous Office Actions.

Carloganu shows a processor that supports two operation modes, normal and isolated (or ring O

as amended).

With respect to applicant's second argument on page 12, "In addition claim 81 recites

that the processor supports one or more higher ring operating modes". The higher ring operating

modes were added with amendment, therefore this argument is moot and the below new grounds

of rejection apply.

With respect to applicant's third argument on page 12, "Furthermore, the processor

comprises an access checking circuit that prevents access to an isolated memory area of the

processing system if the process is not set to operate in the isolated execution mode". The Office

disagrees see '749 col. 2, lines 13-31. Which explain how access to secure resources is only

allowed when using predefined commands. In addition see '749 col. 10, lines 12-26 "The

security model can also process regular (or free) commands when a secured command turns off

the security of the system to allow free access to secured resources". In addition the below

rejection which includes U.S. Patent No. 5,684,948 (hereinafter '948), also clearly shows an

access checking circuit in col. 1, lines 55-67.

With respect to applicant's fourth argument on page 12, "Carloganu says nothing about

determining whether a command involves access to memory". The Office disagrees this

argument does not carry much weight. A memory in inherent in a processor, resource, or

module which Carloganu controls the access to. In addition the reference '948 also shows

involves access to memory, throughout as well as col. 1, lines 31-35.

With respect to applicant's fifth argument on page 12, "Carloganu also says nothing

about disallowing transaction, based on the type of memory are to be accessed and the current

setting of the processor". The Office disagrees see '749 col. 2, lines 35-67. In this passage

Carloganu explains the procedures for operating a set of control resources under the control a

secure processor. Also in the passage Carloganu states: "command primitive associated with the

command code in each of the secured commands is then executed if and only if" this passage has

the same meaning as disallowing transactions.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   **Claims 61-90** are rejected under 35 U.S.C. 103(a) as being unpatentable over Carloganu et al. U.S. Patent No. 6,226,749 (hereinafter '749) in further view of Johnson et al. U.S. Patent No. 5,684,948 (hereinafter '948).

As to independent claim 61,   "A method comprising: detecting a transaction that requests access to a memory of a processing system" is taught in '749 col. 4, lines 44-63 "The secure processor apparatus control the operation of a set of secure processor resources in response to commands communicated thereto from a separate application processing unit" (Note the memory is the resources);

"wherein the processing system comprises a processor that can be set to operate in a normal execution mode in a ring O operating mode and, alternatively, to operate in an isolated execution mode in the ring O operating mode" is shown in '749 col. 3, lines 30-59 "A currently preferred embodiment of this invention incorporates a feature of a command set up table and associated elements which provide added flexibility in that each of the defined commands can be treated as either a secured command or a non-secured command";

"and disallowing the transaction if the transaction requests access to an isolated memory area of the processing system and the processor is not set to operate in the isolated execution mode" is disclosed in '749 col. 10, lines 12-26 "The security module can also process regular (or free) commands when a secured command turns off the security of the system to

allow free access to secured resources or when the command set up table allows such

processing";

the following is not taught in '749 **"wherein the processor also supports one or more higher**

ring operating modes" however '948 teaches "In order to simulate processor privilege levels

for each of a plurality of processor address space segments, current privilege level circuitry holds

a current privilege level access indication, and programmable circuitry associated with each of

the address space segments holds a privilege level access indication associated that address space

segment" in col. 1, line 55 through col. 2, line 12.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to modify a security processor taught in '749 to include support for multiple privilege or security

levels. One of ordinary skill in the art would have been motivated to perform such a

modification because to improve security functions see '948 (col. 1, lines 19 et seq.) "Many

processors, particularly those desirable for use in embedded applications, are not designed to

support multiple "privilege" levels. This may be because most embedded applications do not

require security functions. However, some embedded applications, such as cryptography, do

require security functions. One way to provide these security functions with such a processor is

to completely redesign the processor to support multiple privilege levels. But this would

increase the time to market for those secure embedded applications".

As to dependent claim 62, "wherein: the operation of disallowing the transaction

comprises preventing access to the isolated memory area when the processor is not set to

operate in the isolated execution mode; and the method further comprises allowing access

to the isolated memory area when the processor is set to operate in the isolated execution

mode" is taught in '749 col. 10, lines 12-26.

As to dependent claim 63, "further comprising: creating the isolated memory area

in the memory of the processing system, based at least in part on configuration parameters

for defining the isolated memory area" is shown in '749 col. 3, line 30 through col. 4, line 13

"A currently preferred embodiment of this invention incorporates a feature of a command set up

table and associated elements which provide added flexibility in that each of the defined

commands can be treated as either a secured command or a non-secured command ...c. defining

a set of command format for the commands including at least a command sequence ID, a

command code, and a set of command data items ... testing the authenticity of the secured

command based on the value of at least one element of the secured command using the command

authentication means, i.2.b. testing the regularity of the secured command based on the value of

the command sequence ID".

As to dependent claim 64, "further comprising: creating the isolated memory area

in the memory of the processing system, based at least in part on configuration parameters

for the isolated memory area; and determining whether the transaction requests access to

the isolated memory area, based at least in part on access information for the transaction

and one or more of the configuration parameters for the isolated memory area" is disclosed

in '749 col. 4, lines 44-63 "The application processing unit stores an application software

program comprising a sequence of commands and having or of a pair of predefined command

formats".

As to dependent claim 65, "comprising: determining whether the processor is set to operate in the isolated execution mode, based at least in part on an isolated execution mode setting for the processor" is taught in '749 col. 5, lines 1-30 "a memory portion storing a command set up table including for each of the commands in the set of commands a command type flag having a first value if the command is to be process as a secured command and a second value if the command is to be processed as a non-secured command".

As to dependent claim 66, "wherein: the processor comprises a processor control register to store an isolated execution mode setting; and the method comprises determining whether the processor is set to operate in the isolated execution mode, based at least in part on the isolated execution mode setting from the processor control register" is shown in '749 col. 8, lines 34-67 "For example, in an embodiment in which command sequence is required to be sequential and the security module itself track the Nxt_Seq_ID, the command sequence ID can be encrypted as part of the step of preparing an application software program ... if the Seq_ID for current command, tracked in the security module, matches the expected Nxt_Seq_ID which is generally part of the previous secured command".

As to dependent claim 67, "further comprising: allowing the transaction to succeed if the processor is set to operate in the isolated execution mode" is disclosed in '749 col. 9, lines 20-39 "FIG. 9 illustrates a Verify CMD_Auth routing which is used in an embodiment which uses a secured command format in which each command includes an S_MAC_Val in the form of a message authentication code (MAC) signature based on subjecting a predefined portion of the command".

As to dependent claim 68, "further comprising: if the processor is set to operate in the isolated execution mode, asserting a signal from the processor to grant access for the transaction" is taught in is shown in '749 col. 9, lines 20-39.

As to dependent claim 69, "wherein: the transaction that requests access to the memory of the processing system comprises an access transaction generated during execution of an instruction in the processor" is disclosed in '749 col. 7, lines 33-42 "Application processing unit 60 stores a application software program 61 which includes a plurality of secured commands that are sent to security module 50 where they are processed using secured command processing routing 51 which will invoke operation of associated command primitives if the command passes sequence and authenticity testing".

As to dependent claim 70. A method according to claim 61, wherein: the transaction that requests access to the memory of the processing system comprises an access transaction involving one or more resources selected from the group consisting of: a front side bus (FSB); and a translation lookaside buffer (TLB)" is taught in '749 col. 4, lines 44-67 and col. 9, lines 57-67 "In this routing, the diffence is that the Nxt_Seq_ID from the command itself is stored in the buffer that is provided in the security module·for that parameter if the sequence verification testing step returns YES".

As to independent claim 71, this claim is direct to an apparatus of the method of claim 61; therefore it is rejected along similar rationale.

As to dependent claims 72-80, these claims contain substantially similar subject matter as claim 62-70; therefore they are rejected along similar rationale.

As to independent claim **81,** this claim is direct to the processing system of the method

of claim 61; therefore it is rejected along similar rationale.

As to dependent claims **82-90,** these claims contain substantially similar subject matter

as claim 62-70; therefore they are rejected along similar rationale.
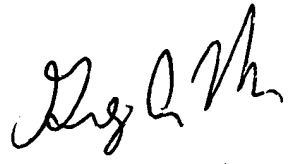

Conclusion

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ellen C Tran whose telephone number is

(571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the

organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
3 August 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100